RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: LAB1-W08

Hack Proof Cloud Based Applications—Integrate Cloud Based Protection

Jason Lam
SANS Institute
https://www.linkedin.com/in/jasonlam-security/

Serge Borso
SANS Institute
https://www.linkedin.com/in/sergeborso/

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Agenda

- Introduction to applications in the cloud
- Security Challenges
  - Lab 0 – Introduction to the test environment
  - Lab 1 – Web and API Vulnerabilities
  - Lab 2 – WAF Defenses
  - Lab 3 – API Gateway
  - Lab 4 – Logging

Applications Moving To The Cloud

- Moving applications using a "lift and shift" approach is common
- Refactor/rebuild with cloud native pattern is not always possible
- How do we gain security benefits rapidly by moving to the cloud?
- Low effort, high benefit strategy
  - Resulting in significant security enhancements made possible by cloud-native services

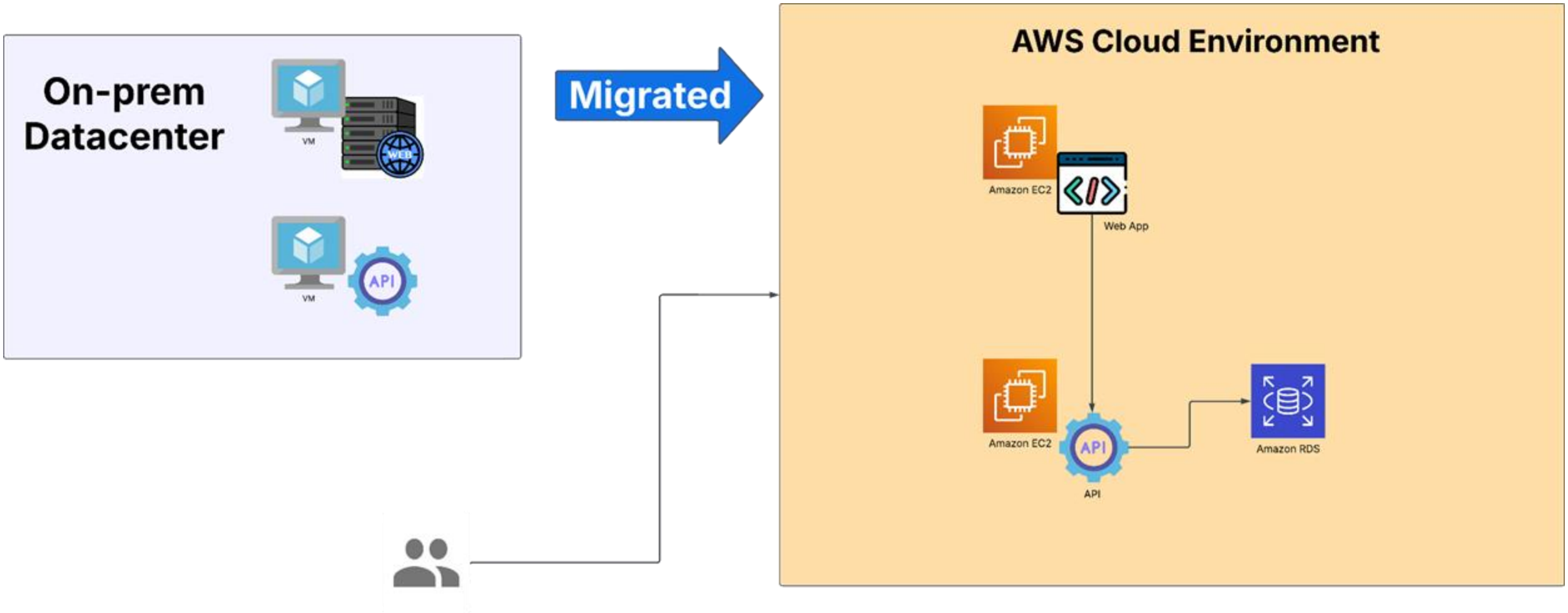
Application And API Attacks

- API1:2023 - Broken Object Level Authorization
- API2:2023 - Broken Authentication
- API3:2023 - Broken Object Property Level Authorization
- API4:2023 - Unrestricted Resource Consumption
- API5:2023 - Broken Function Level Authorization
- API6:2023 - Unrestricted Access to Sensitive Business Flows
- API7:2023 - Server Side Request Forgery
- API8:2023 - Security Misconfiguration
- API9:2023 - Improper Inventory Management
- API10:2023 - Unsafe Consumption of APIs

Security Benefits With Cloud

- Managed environment (PaaS, SaaS)
- Easy to integrate and adopt
  - WAF and runtime protection (CWPP)
  - IAM Integration
  - Enhanced Logging
  - API throttling and filtering
- Vulnerability Scanning
- CI/CD pipeline (IaC and DevSecOps)

Environment Diagram (Before and After)



RSAC 2025 Conference

Lab 0

Understanding Our Cloud Environment

Follow Instructions Here: https://sansrsac.com

Debrief Lab 0: Our Cloud Environment

- Understanding our cloud environment
  - EC2 instances (Virtual Machines)
  - Web Application
  - Database (Relational Database Service (RDS))
  - API
- Understanding our attack surface
  - What can an adversary attack, and how can they cause harm?

RSAC 2025 Conference

Lab 1

Web Application Vulnerabilities

Follow Instructions Here: https://sansrsac.com

Debrief Lab 1: Application Vulnerabilities

- Explored Web vulnerabilities
- Design and coding fixes required
- Flaws can lead to data exposure, compromise of the application environment
- Think - How do we improve the security posture of our application quickly?

RSAC 2025 Conference

Lab 2

Web Application Firewall (WAF) Integration

Follow Instructions Here: https://sansrsac.com

Debrief Lab 2: Web Application Firewall

- Quickly able to provide tactical defenses to our web application
- Works "OK" for common web vulnerabilities
- Requires configuration tuning to work effectively
- Not a perfect defense solution, comprehensive coding and design fix still required
- Treat it as a defense in depth component

RSAC 2025 Conference

Lab 3

API Gateway Integration

Follow Instructions Here: https://sansrsac.com

Debrief Lab 3: API Gateway

- API endpoints are meant to be lightweight
- API gateways provide crucial security capabilities to the APIs
- Similar to the WAF, it's a defense in depth component
- Does not replace secure coding
- Still critically important to design APIs securely

RSAC 2025 Conference

Lab 4

Cloud Logging

Follow Instructions Here: https://sansrsac.com

Debrief Lab 4: Cloud Logging

- Logging provides important visibility into security events
- Log consolidation is crucial to understand security events in the environment
- Cloud service providers provide great logging and log processing capabilities
- Infrastructure and application logs are both useful to piece together the big picture

What do you do next?

- Next week you should:
  - Review the applications in your organization's cloud environment
  - Identify misconfiguration and vulnerabilities
- In the first three months following this presentation you should:
  - Plan and deploy security enhancements via automation to your cloud applications
  - Validate security controls were properly implemented
- Within six months you should:
  - Refactor applications to leverage cloud native security patterns and tools

RSAC 2025 Conference

Many Voices.
One Community.

Jason Lam
SANS Institute
www.linkedin.com/in/jasonlam-security

Serge Borso
SANS Institute
www.linkedin.com/in/sergeborso